

WHAT IS CLAIMED IS:

1. An integrated security and communications system comprising:
 - a security controller having at least one sensory input, at least one alarm output and at least one control signal input/output port;
 - a control interface operatively connected to said at least one control signal input/output port; and
 - 10 a communications unit connected to a communication channel for providing at least one communication function, a first communication port for connection to one of said at least one control signal input/output port of said security controller for
 - 15 providing at least one of said at least one communication function to a user at said control interface, and a second communication port for connection to a communication device at which said at least one communication function is provided to said
 - 20 user.
2. The system of claim 1 wherein:
 - said communication channel comprises a telephone line; and
 - said communication device comprises a
 - 5 telephone.
3. The system of claim 2 wherein said at least one communication function comprises telephony.
4. The system of claim 1 wherein:
 - said communication channel comprises an Internet connection;
 - said communication device comprises a
 - 5 computer; and

FILED 19350000

30 at said at least one user control interface for
uniquely identifying each of at least one of said
authorized users, wherein:

a particular one of said at least one
authorized user initiates said state consistent with
35 presence of an authorized user by activating said
authorization unit using an indicium unique to said
particular authorized user; and

said telephone interface unit presents
for access, at said user control interface, only voice
40 mail functions for which said particular authorized
user is authorized.

7. The security system of claim 6 wherein:
said authorization unit comprises a
keypad at said user control interface;
said indicium comprises a respective
5 passcode unique to each said at least one authorized
user; and

said activating of said authorization
unit comprises entering said passcode on said keypad.

8. The security system of claim 6 wherein:
said authorization unit comprises a
receiver at said user control interface;
said indicium comprises a respective
5 transmitter uniquely coded to each said at least one
authorized user; and

said activating of said authorization
unit comprises actuating said transmitter within
communication range of said receiver.

9. The security system of claim 8 wherein
said receiver and said coded transmitter are wireless.

10. The security system of claim 6 wherein:

FOUO - 1330000

said authorization unit comprises a token reader at said user control interface;

said indicium comprises a respective
5 coded token unique to each said at least one authorized user; and

said activating of said authorization unit comprises presenting said token to said token reader.

11. The security system of claim 6 wherein said voice mail functionality is activated automatically upon entry of said system into said state consistent with presence of an authorized user on said
5 premises.

12. The security system of claim 6 wherein said telephone interface unit further comprises a remote access unit through which a user remotely controls, during a single telephone call session to
5 said system from a remote location, both (a) at least one security system control function, and (b) at least one voice mail function.

13. The security system of claim 6 further comprising at least one telephone set connected to said telephone line; wherein:

said voice mail functionality comprises
5 playback of an outgoing message to an incoming caller;

said telephone interface unit further provides a call screening function at at least one of (a) said at least one telephone set, and (b) said at least one user control interface, said user control
10 interface including a speaker; and

said call screening function is full-duplex, allowing said incoming caller to speak an

announcement that is audible at said speaker during said playback of said outgoing message.

14. The security system of claim 6 further comprising at least one telephone set connected to said telephone line; wherein:

5 said telephone interface unit further provides an aural indication at said at least one telephone set when a voice mail message has been received and is awaiting playback.

15. The security system of claim 6 further comprising at least one telephone set connected to said telephone line, said least one telephone set having a ringer; wherein:

5 said user control interface includes a speaker; and

 said telephone interface unit further provides:

10 a privacy function whereby said ringer can be deactivated under control of a user, and
 as part of said privacy function, a privacy breakthrough function whereby a caller issues a command when said privacy function is active for broadcasting a message on said speaker.

16. The security system of claim 6 wherein said voice mail functionality includes a toll saver feature controlled by said state of said system.

17. The security system of claim 16 wherein said toll saver feature is active only when said state of said system indicates absence of authorized users from said premises.

18. The security system of claim 17 wherein said toll saver feature can further be controlled by a user at said user control interface.

19. The security system of claim 18 further comprising at least one telephone set connected to said telephone line; wherein:

5 said toll saver feature can be controlled by a user at at least one of said at least one telephone set.

20. The security system of claim 6 wherein said telephone interface unit further comprises:

5 a calling party identification unit for displaying calling party identification data, said calling party identification data being displayed at said user control interface; and

10 a distinctive ringing generator responsive to said calling party identification data for generating a distinctive ringing signal different from a standard incoming ringing signal based on said calling party identification data.

21. The security system of claim 20 wherein said distinctive ringing generator generates a first number of distinctive ringing signals, each distinctive ringing signal in said first number of distinctive ringing signals identifying at least one preselected calling party from a second number of preselected calling parties.

22. The security system of claim 21 wherein said first number is equal to said second number, whereby each distinctive ringing signal is associated with a unique preselected calling party.

TO: "4959360"

23. The security system of claim 21 wherein said first number is less than said second number, whereby each distinctive ringing signal is associated with a plurality of said preselected calling parties.

24. The security system of claim 21 wherein said distinctive ringing generator comprises a ringing signal interrupter for interrupting said standard incoming ringing signal in a second number of ways
5 equal to said second number of distinctive ringing signals, to produce said second number of distinctive ringing signals.

25. The security system of claim 20 wherein said distinctive ringing generator comprises a ringing signal interrupter for interrupting said standard incoming ringing signal to produce said distinctive
5 ringing signal.

26. The security system of claim 6 wherein said telephone interface unit further comprises:

a calling party identification unit for displaying calling party identification data, said
5 calling party identification data being displayed at said user control interface;

memory for storing instructions for paging a user when said calling party identification data identifies one of at least one particular calling
10 party; and

a processor for acting on said instructions and placing a call to a user's pager when said calling party identification data identify one of said at least one particular calling party.

27. The security system of claim 6 further comprising at least one telephone set connected to said

telephone line through said telephone interface unit;
wherein:

5 at least one of said at least one user
control interface comprises a speaker;

 said telephone interface unit further
comprises a public address function; whereby, when a
user issues a command at said telephone set:

10 said telephone set is disconnected from
said telephone line and connected to said speaker of
said at least one of said at least one user control
interface.

28. The security system of claim 27 wherein
said telephone set is connected to said speaker of each
said at least one of said at least one user control
interface.

29. The security system of claim 27 wherein,
on command of said user, said telephone set is
connected to said speaker of any one or more of said at
least one of said at least one user control interface.

30. The security system of claim 27 wherein,
when said user issues said command at said telephone
set, said telephone interface unit maintains said
telephone line in an off-hook condition while said
5 public address function is in use.

31. The security system of claim 6 further
comprising at least one telephone set connected to said
telephone line through said telephone interface unit;
wherein:

5 at least one of said at least one user
control interface comprises a microphone;

said telephone interface unit further comprises a room monitor function; whereby, when a user issues a command at said telephone set:

10 said telephone set is disconnected from said telephone line and connected to said microphone of said at least one of said at least one user control interface.

32. The security system of claim 6 further comprising at least one telephone set connected to said telephone line through said telephone interface unit; wherein:

5 at least one programmable parameter of said security system is programmable:
 (a) at said at least one user control interface;
 (b) at said connected telephone set; and
10 (c) remotely by calling into said system on said telephone line.

33. The security system of claim 32 wherein:
 there are a plurality of said programmable parameters; and

 only a subset of said plurality of
5 programmable parameters is programmable remotely.

34. The security system of claim 6 further comprising at least one user-controlled processor connected via a modem to said telephone line through said telephone interface unit; wherein:

5 at least one programmable parameter of said security system is programmable;
 said telephone interface unit includes a control signal detector for detecting control signals sent from said user-controlled processor through said
10 modem; whereby:

responsive to said control signals from said user-controlled processor, said telephone interface unit disconnects from said telephone line and enters a user-controlled mode.

35. The security system of claim 34 wherein in said user-controlled mode said user-controlled processor performs any one of:

- programming said at least one
- 5 programmable parameter of said security system;
- downloading voice mail messages received as part of said voice mail functionality from said telephone interface unit to said user-controlled processor; and
- 10 uploading voice prompts composed at said user-controlled processor to said telephone interface unit.

36. The security system of claim 34 wherein said user-controlled processor comprises a personal computer.

37. The security system of claim 6 wherein:
- said telephone line has central office voice mail associated therewith; and
 - said voice mail functionality comprises
 - 5 indicating a central office voice message waiting.

38. The security system of claim 37 wherein said indicating central office message waiting comprises providing an indication at said user control interface.

39. The security system of claim 38 wherein said indication at said user control interface is visual.

40. The security system of claim 38 wherein said indication at said user control interface is aural.

41. The security system of claim 37 further comprising at least one telephone set connected to said telephone line; wherein:

5 said indicating central office message waiting comprises providing an indication at said telephone set.

42. The security system of claim 41 wherein said indication at said telephone set is aural.

43. The security system of claim 41 wherein: said telephone set includes a visual indicator; and

5 said indication at said telephone set is visual.

44. The security system of claim 6 wherein said telephone interface unit further comprises a remote access unit through which a user controls at least one security system control function via said
5 telephone line.

45. The security system of claim 44 wherein said user, through said remote access unit, controls said at least one security system function from a telephone at a remote location by calling into said
5 telephone line from said remote location.

46. The security system of claim 44 further comprising at least one telephone set connected to said telephone line; wherein:

5 said user, through said telephone
interface unit, controls said at least one security
system function from said telephone set.

47. The security system of claim 6 further
comprising at least one telephone set connected to said
telephone line; wherein:

5 said telephone interface unit monitors
said telephone line and, when an outgoing telephone
call is placed on said at least one telephone set, logs
said outgoing telephone call.

48. The security system of claim 47 wherein:
said telephone interface unit comprises
memory for storing data identifying numbers to which
outgoing calls are restricted; and

5 when an outgoing call is placed on said
telephone set to one of said numbers to which outgoing
calls are restricted, said telephone interface unit
prevents said outgoing call from being completed.

49. The security system of claim 48 wherein:
said memory further stores at least one
user code; and

5 when said user code is entered during
said outgoing call, said telephone interface unit
allows said outgoing call to be completed to one of
said numbers to which outgoing calls are restricted.

50. The security system of claim 6 wherein
said user control interface is connected to an external
data network for at least one of (a) sending, and
(b) receiving, data.

51. The security system of claim 50 wherein:
said data comprise electronic mail; and

access to said electronic mail is restricted based on said state of said system.

52. The security system of claim 51 wherein said electronic mail is accessible when said state is consistent with presence of an authorized user on said premises.

53. The security system of claim 52 having a plurality of authorized users, wherein:

when a particular authorized user initiates said state consistent with presence of an
5 authorized user by activating said authorization unit, said user control interface presents, for access at said user control interface, only electronic mail addressed to said particular authorized user.

54. The security system of claim 53 wherein:
said authorization unit comprises a keypad at said user control interface;
said indicium comprises a passcode
5 unique to said particular authorized user; and
said activation of said authorization unit comprises entry of said passcode at said keypad.

55. The security system of claim 53 wherein:
said authorization unit comprises a receiver;
said indicium comprises a transmitter
5 coded uniquely to said particular authorized user; and
said activation of said authorization unit comprises activation of said coded transmitter in communication range of said receiver.

56. The security system of claim 55 wherein said receiver and said coded transmitter are wireless.

said indicium comprises a token coded

said activation of said authorization

when a particular authorized user

initiates said state consistent with presence of an

said indicium comprises a passcode

unique to said particular authorized user; and

said indicium comprises a transmitter

said activation of said authorization

unit comprises activation of said coded transmitter in communication range of said receiver.

62. The security system of claim 58 wherein:
said authorization unit comprises a
token reader;

5 uniquely to said particular authorized user; and
said activation of said authorization
unit comprises presentation of said coded token to said
reader.

63. The security system of claim 50 wherein:
said data comprise electronic mail;
said system has at least one authorized
user; and

5 when one of said at least one authorized
user enters a security system command at said user
control interface by activating said authorization
unit, said user control interface sends an electronic
mail message to a predetermined recipient advising of
10 said entry of said command by said one of said at least
one authorized user.

64. The security system of claim 63 wherein:
said authorization unit comprises a
keypad at said user control interface;
said indicium comprises a passcode
5 unique to said one of said at least one authorized
user; and

said activation of said authorization unit comprises entry of said passcode at said keypad.

65. The security system of claim 63 wherein:

said authorization unit comprises a receiver;

5 said indicium comprises a transmitter
coded uniquely to said one of said at least one
authorized user; and

 said activation of said authorization
unit comprises activation of said coded transmitter in
communication range of said receiver.

66. The security system of claim 65 wherein
said receiver and said coded transmitter are wireless.

67. The security system of claim 63 wherein:
 said authorization unit comprises a
token reader;

5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; and

 said activation of said authorization
unit comprises presentation of said coded token to said
reader.

68. The security system of claim 50 wherein:
 said external data network is the
Internet;

5 said data comprise World Wide Web pages;
 said system has at least one authorized
user; and

 when one of said at least one authorized
user enters a security system command at said user
control interface by activating said authorization
10 unit, said system retrieves a World Wide Web page
directed to said one of said at least one authorized
user and displays said World Wide Web page at said user
control interface.

00000000-00000000

69. The security system of claim 68 wherein:
said authorization unit comprises a
keypad;
said indicium comprises a passcode
5 unique to said one of said at least one authorized
user; and
said activation of said authorization
unit comprises entry of said passcode at said keypad.
70. The security system of claim 68 wherein:
said authorization unit comprises a
receiver;
said indicium comprises a transmitter
5 coded uniquely to said one of said at least one
authorized user; and
said activation of said authorization
unit comprises activation of said coded transmitter in
communication range of said receiver.
71. The security system of claim 70 wherein
said receiver and said coded transmitter are wireless.
72. The security system of claim 70 wherein:
said transmitter is encoded with
multiple codes;
said activation of said authorization
5 unit comprises activation of a selected one of said
multiple codes by said one of said at least one
authorized user; and
said system retrieves a different World
Wide Web page based on which of said multiple codes has
10 been selected.
73. The security system of claim 68 wherein:
said authorization unit comprises a
token reader;

606344-1350300

5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; and

 said activation of said authorization
unit comprises presentation of said coded token to said
reader.

74. The security system of claim 50 wherein:
 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface by activating said authorization unit;

 said external data network is the
Internet; and

10 said activation of said authorization
unit logs said one of said at least one authorized user
onto the Internet at said user control interface.

75. The security system of claim 50 wherein:
 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface by activating said authorization unit using
an indicium unique to said one of said at least one
authorized user;

10 said one of said at least one user uses
said external data network to access a financial
institution to perform a financial transaction;

 said indicium is registered with said
financial institution as an identifier of said one of
said at least one authorized user; and

15 said indicium is sent to said financial
institution as part of said financial transaction.

FILED OCT 13 1990

76. The security system of claim 50 wherein functions of said system are remotely accessible via said external data network.

77. The security system of claim 50 wherein:
said system transmits security data signals to a central communication station via said external data network and said alternate channel and
5 awaits acknowledgment thereof; and

when said acknowledgment arrives from a first one of said external data network and said alternate channel, said system terminates transmission of said security data on a second one of said external
10 data network and said alternate channel.

78. The security system of claim 77 wherein:
one of said external data network and said alternate channel normally operates faster than another of said external data network and said
5 alternate channel; and

said system begins transmission of said security data signals on said one of said external data network and said alternate channel before beginning transmission of said security data signals on said
10 another of said external data network and said alternate channel.

79. The security system of claim 77 further comprising a firewall between said user control interface and said external data network; wherein:
said firewall allows only communication
5 originating at said system and prevents communication originating on said external data network; and
to receive said acknowledgment from said central communication station, said system initiates communication with said external data network so that

5

5

5

5

5

5

5

84. The security system of claim 50 wherein said system accepts commands from a user via said external data network.

85. The security system of claim 84 further comprising a firewall between said user control interface and said external data network; wherein:

5 said firewall allows only communication
originating at said system and prevents communication
originating on said external data network; and
to receive said commands from said user,
said system initiates communication with said external
data network so that said firewall allows said
10 communication, said initiated communication including a
query to said external data network for commands issued
by said user to be communicated from said external data
network to said system.

86. The security system of claim 50 wherein
said system sends security data signals to
predetermined recipients via said external data
network.

87. The security system of claim 50
comprising more than one of said user control
interface, each said user control interface functioning
as an independent terminal of said external data
5 network.

88. The security system of claim 50 further
comprising a firewall between said user control
interface and said external data network; wherein:
said firewall allows only communication
5 originating at said system and prevents communication
originating on said external data network; and
to receive data, said system initiates
communication with said external data network so that
said firewall allows said communication, said initiated
10 communication including a query to said external data

98. The security system of claim 94 wherein:
said user control interface comprises a
token reader;

5 said indicium comprises a token uniquely
coded to each of said at least one authorized user; and
 said activating of said authorization
unit comprises presentation of said coded token to said
reader.

99. The security system of claim 93 having a
plurality of authorized users, and having an
authorization unit for uniquely identifying each of at
least one of said authorized users, wherein:

5 a particular authorized user initiates
said state consistent with presence of an authorized
user by activating said authorization unit using an
indiciu unique to said particular authorized user; and
 said user control interface presents
10 access at said user control interface to electronic
mail message sending from said particular authorized
user.

100. The security system of claim 99 wherein:
said user control interface comprises a
keypad;

5 said indicium comprises a respective
passcode unique to each of said at least one authorized
user; and

 said activation of said authorization
unit indicium comprises entry of said passcode at said
keypad.

101. The security system of claim 99 wherein:
said user control interface comprises a
receiver;

100-101-102-103-104-105-106-107-108-109-110-111-112-113-114-115-116-117-118-119-120-121-122-123-124-125-126-127-128-129-130-131-132-133-134-135-136-137-138-139-140-141-142-143-144-145-146-147-148-149-150-151-152-153-154-155-156-157-158-159-160-161-162-163-164-165-166-167-168-169-170-171-172-173-174-175-176-177-178-179-180-181-182-183-184-185-186-187-188-189-190-191-192-193-194-195-196-197-198-199-200-201-202-203-204-205-206-207-208-209-210-211-212-213-214-215-216-217-218-219-220-221-222-223-224-225-226-227-228-229-230-231-232-233-234-235-236-237-238-239-240-241-242-243-244-245-246-247-248-249-250-251-252-253-254-255-256-257-258-259-260-261-262-263-264-265-266-267-268-269-270-271-272-273-274-275-276-277-278-279-280-281-282-283-284-285-286-287-288-289-290-291-292-293-294-295-296-297-298-299-300-301-302-303-304-305-306-307-308-309-310-311-312-313-314-315-316-317-318-319-320-321-322-323-324-325-326-327-328-329-330-331-332-333-334-335-336-337-338-339-340-341-342-343-344-345-346-347-348-349-350-351-352-353-354-355-356-357-358-359-360-361-362-363-364-365-366-367-368-369-370-371-372-373-374-375-376-377-378-379-380-381-382-383-384-385-386-387-388-389-390-391-392-393-394-395-396-397-398-399-400-401-402-403-404-405-406-407-408-409-410-411-412-413-414-415-416-417-418-419-420-421-422-423-424-425-426-427-428-429-430-431-432-433-434-435-436-437-438-439-440-441-442-443-444-445-446-447-448-449-450-451-452-453-454-455-456-457-458-459-460-461-462-463-464-465-466-467-468-469-470-471-472-473-474-475-476-477-478-479-480-481-482-483-484-485-486-487-488-489-490-491-492-493-494-495-496-497-498-499-500-501-502-503-504-505-506-507-508-509-510-511-512-513-514-515-516-517-518-519-520-521-522-523-524-525-526-527-528-529-530-531-532-533-534-535-536-537-538-539-540-541-542-543-544-545-546-547-548-549-550-551-552-553-554-555-556-557-558-559-560-561-562-563-564-565-566-567-568-569-570-571-572-573-574-575-576-577-578-579-580-581-582-583-584-585-586-587-588-589-590-591-592-593-594-595-596-597-598-599-600-601-602-603-604-605-606-607-608-609-610-611-612-613-614-615-616-617-618-619-620-621-622-623-624-625-626-627-628-629-630-631-632-633-634-635-636-637-638-639-640-641-642-643-644-645-646-647-648-649-650-651-652-653-654-655-656-657-658-659-660-661-662-663-664-665-666-667-668-669-670-671-672-673-674-675-676-677-678-679-680-681-682-683-684-685-686-687-688-689-690-691-692-693-694-695-696-697-698-699-700-701-702-703-704-705-706-707-708-709-710-711-712-713-714-715-716-717-718-719-720-721-722-723-724-725-726-727-728-729-730-731-732-733-734-735-736-737-738-739-740-741-742-743-744-745-746-747-748-749-750-751-752-753-754-755-756-757-758-759-760-761-762-763-764-765-766-767-768-769-770-771-772-773-774-775-776-777-778-779-780-781-782-783-784-785-786-787-788-789-790-791-792-793-794-795-796-797-798-799-800-801-802-803-804-805-806-807-808-809-810-811-812-813-814-815-816-817-818-819-820-821-822-823-824-825-826-827-828-829-830-831-832-833-834-835-836-837-838-839-840-841-842-843-844-845-846-847-848-849-850-851-852-853-854-855-856-857-858-859-860-861-862-863-864-865-866-867-868-869-870-871-872-873-874-875-876-877-878-879-880-881-882-883-884-885-886-887-888-889-890-891-892-893-894-895-896-897-898-899-900-901-902-903-904-905-906-907-908-909-910-911-912-913-914-915-916-917-918-919-920-921-922-923-924-925-926-927-928-929-930-931-932-933-934-935-936-937-938-939-940-941-942-943-944-945-946-947-948-949-950-951-952-953-954-955-956-957-958-959-960-961-962-963-964-965-966-967-968-969-970-971-972-973-974-975-976-977-978-979-980-981-982-983-984-985-986-987-988-989-990-991-992-993-994-995-996-997-998-999-1000

said activation of said authorization unit comprises activation of said coded transmitter in communication range of said receiver.

103. The security system of claim 99 wherein:
said user control interface comprises a
token reader;

104. The security system of claim 89 wherein:
said data comprise electronic mail;
said system has at least one authorized
user, and has an authorization unit for uniquely
5 identifying each of at least one of said authorized
users; and

105. The security system of claim 104
wherein:

said user control interface comprises a keypad;

5 said indicium comprises a respective passcode unique to each of said at least one authorized user; and

 said activation of said authorization unit comprises entry of said passcode at said keypad.

106. The security system of claim 104 wherein:

 said user control interface comprises a receiver;

5 said indicium comprises a respective transmitter uniquely coded for each of said at least one authorized user; and

 said activation of said authorization unit comprises activation of said coded transmitter in
10 communication range of said receiver.

107. The security system of claim 106 wherein said receiver and said coded transmitter are wireless.

108. The security system of claim 104 wherein:

 said user control interface comprises a token reader;

5 said indicium comprises a token uniquely coded to each of said at least one authorized user; and
 said activation of said authorization unit comprises presentation of said coded token to said reader.

109. The security system of claim 89 wherein:
 said external data network is the

Internet;

 said data comprise World Wide Web pages;

Approved for Release by NSA on 09-08-2013 pursuant to E.O. 13526

5 said system has at least one authorized user, and has an authorization unit for uniquely identifying each of at least one of said authorized users; and

 when one of said at least one authorized
10 user enters a security system command at said user control interface by activating said authorization unit using an indicium unique to said one of said at least one authorized user, said system retrieves a World Wide Web page directed to said one of said at least one
15 authorized user and displays said World Wide Web page at said user control interface.

110. The security system of claim 109
wherein:

 said user control interface comprises a keypad;

5 said indicium comprises a respective passcode unique to each of said at least one authorized user; and

 said activation of said authorization unit comprises entry of said passcode at said keypad.

111. The security system of claim 109
wherein:

 said user control interface comprises a receiver;

5 said indicium comprises a respective transmitter uniquely coded for each of said at least one authorized user; and

 said activation of said authorization unit comprises activation of said coded transmitter in
10 communication range of said receiver.

112. The security system of claim 111 wherein
said receiver and said coded transmitter are wireless.

113. The security system of claim 111
wherein:

said respective transmitter is encoded
with multiple codes;

5 said activation of said authorization
unit comprises activation of a selected one of said
multiple codes by said one of said at least one
authorized user; and

10 said system retrieves a different World
Wide Web page based on which of said multiple codes has
been selected.

114. The security system of claim 109
wherein:

said user control interface comprises a
token reader;

5 said indicium comprises a respective
token uniquely coded for each of said at least one
authorized user; and

10 said activation of said authorization
unit comprises presentation of said coded token to said
reader.

115. The security system of claim 89 wherein:

5 said system has at least one authorized
user, and has an authorization unit for uniquely
identifying each of at least one of said authorized
users;

one of said at least one authorized user
activates said authorization unit using an indicium
unique to said one of said at least one authorized
user;

10 said external data network is the
Internet; and

116. The security system of claim 89 wherein:
said system has at least one authorized
user, and has an authorization unit for uniquely
identifying each of at least one of said authorized
5 users;

said one of said at least one user uses
said external data network to access a financial
institution to perform a financial transaction;

said indicium is sent to said financial institution as part of said financial transaction.

118. The security system of claim 89 wherein:
said system transmits security data
signals to a central communication station via said
external data network and an alternate channel and
5 awaits acknowledgment thereof; and

when said acknowledgment arrives from a first one of said external data network and said alternate channel, said system terminates transmission

of said security data on a second one of said external
10 data network and said alternate channel.

119. The security system of claim 118
wherein:

one of said external data network and
said alternate channel normally operates faster than
5 another of said external data network and said
alternate channel; and

said system begins transmission of said
security data signals on said one of said external data
network and said alternate channel before beginning
10 transmission of said security data signals on said
another of said external data network and said
alternate channel.

120. The security system of claim 118 further
comprising a firewall between said user control
interface and said external data network; wherein:

said firewall allows only communication
5 originating at said system and prevents communication
originating on said external data network; and

to receive said acknowledgment from said
central communication station, said system initiates
communication with said external data network so that
10 said firewall allows said communication, said initiated
communication including a query to said external data
network for said acknowledgment to be communicated from
said central communication station to said system.

121. The security system of claim 120 wherein
said query to said external network comprises a query
to said central communication station.

122. The security system of claim 118 wherein
said alternate channel is said telephone line.

123. The security system of claim 118
wherein:

said system transmits security data
signals to a central communication station via a
5 plurality of channels; and

when said acknowledgment arrives from a
first one of said plurality of channels, said system
terminates transmission of said security data on each
other one of said plurality of channels.

124. The security system of claim 123
wherein:

one of said plurality of channels
normally operates faster than others of said plurality
5 of channels; and

said system begins transmission of said
security data signals on said one of said plurality of
channels before beginning transmission of said security
data signals on said others of said plurality of
10 channels.

125. The security system of claim 89 wherein
said system accepts commands from a user via said
external data network.

126. The security system of claim 125 further
comprising a firewall between said user control
interface and said external data network; wherein:

said firewall allows only communication
5 originating at said system and prevents communication
originating on said external data network; and

to receive said commands from said user,
said system initiates communication with said external
data network so that said firewall allows said
10 communication, said initiated communication including a

query to said external data network for commands issued by said user to be communicated from said external data network to said system.

127. The security system of claim 89 wherein said system sends security data signals to predetermined recipients via said external data network.

128. The security system of claim 89 comprising more than one of said user control interface, each said user control interface functioning as an independent terminal of said external data network.

129. The security system of claim 89 further comprising a firewall between said user control interface and said external data network; wherein:
said firewall allows only communication
5 originating at said system and prevents communication originating on said external data network; and
to receive data, said system initiates communication with said external data network so that said firewall allows said communication, said initiated
10 communication including a query to said external data network for data sought to be communicated from said external data network to said system.

130. A secure communications system comprising:
a first communication station connected to a communication medium;
5 a central communication station connected to said communication medium; and
at least a second communication station connected to said communication medium; wherein:

all communication between said first
10 communication station and said central communication
station is initiated by said first communication
station;

communication between said first
communication station and said second communication
15 station is established by leaving a message for said
first communication station at said central
communication station indicating communication is
desired between said first communication station and
said second communication station; and

20 when said first communication station
initiates communication with said central communication
station, said first communication station receives said
message for said first communication station, maintains
its initiated communication with said central
25 communication station and instructs said central
communication station to relay communications between
said first communication station and said second
communication station.

131. The secure communications system of
claim 130 wherein said message for said first
communication station is left by said second
communication station.

132. The secure communications system of
claim 130 wherein said message for said first
communication station is left by said central
communication station.

133. The secure communications system of
claim 130 wherein:

said first communication station
includes a first firewall between said first

2025 RELEASE UNDER E.O. 14176

5 communication station and said communication medium;
and

said first firewall allows only
communication originating at said first station and
prevents communication originating on said
10 communication medium.

134. The secure communications system of
claim 130 wherein:

said first communication station further
comprises a first station encryption processor for
5 encrypting and decrypting communications using a first
digital key identified with said first station;

said central communication station
further comprises:

a central encryption processor for
10 encrypting and decrypting communications using a
digital key, and

key memory for storing said first
digital key and associating said stored first digital
key with said first communication station;

15 said first communication station uses
said first station encryption processor to encrypt with
said first station digital key each communication sent
to said central communication station, and to decrypt
with said first station digital key each communication
20 received from said central communication station; and

said central communication station uses
said central encryption processor to encrypt with said
first station digital key each communication sent to
said first communication station and to decrypt with
25 said first station digital key each communication
received from said first communication station.

135. The secure communications system of
claim 134 wherein:

all communication between said second communication station and said central communication station is initiated by said second communication station;

communication between said second communication station and said first communication station is established by leaving a message for said second communication station at said central communication station indicating communication is desired between said second communication station and said first communication station; and

when said second communication station
15 initiates communication with said central communication
station, said second communication station receives
said message for said second communication station,
maintains its initiated communication with said central
communication station and instructs said central
20 communication station to relay communications between
said first communication station and said second
communication station.

136. The secure communications system of claim 135 wherein said message for said second communication station is left by said first communication station.

137. The secure communications system of claim 135 wherein said message for said second communication station is left by said central communication station.

138. The secure communications system of
claim 135 wherein:

said second communication station
includes a second firewall between said second

5 communication station and said communication medium;
and

said second firewall allows only
communication originating at said second station and
prevents communication originating on said
10 communication medium.

139. The secure communications system of
claim 135 wherein:

said second communication station
further comprises a second station encryption processor
5 for encrypting and decrypting communications using a
second digital key identified with said second station;
said key memory of said central
communication station further stores said second
digital key and associates said stored second digital
10 key with said second communication station;

said second communication station uses
said second station encryption processor to encrypt
with said second station digital key each communication
sent to said central communication station, and to
15 decrypt with said second station digital key each
communication received from said central communication
station; and

said central communication station uses
said central encryption processor to encrypt with said
20 second station digital key each communication sent to
said second communication station and to decrypt with
said second station digital key each communication
received from said second communication station.

140. The secure communications system of
claim 139 wherein:

said first communication station is a
premises alarm system; and

5 said second communication station is a
central alarm monitoring station.

141. The secure communications system of
claim 139 wherein:

 said first communication station is a
first premises alarm system; and

5 said second communication station is a
second premises alarm system.

142. The secure communications system of
claim 139 wherein:

 said first communication station is a
premises alarm system; and

5 said second communication station is a
remote communications terminal.

143. The secure communications system of
claim 130 wherein:

 all communication between said second
communication station and said central communication
5 station is initiated by said second communication
station;

 communication between said second
communication station and said first communication
station is established by leaving a message for said
10 second communication station at said central
communication station indicating communication is
desired between said second communication station and
said first communication station; and

 when said second communication station
15 initiates communication with said central communication
station, said second communication station receives
said message for said second communication station,
maintains its initiated communication with said central
communication station and instructs said central

2025 RELEASE UNDER E.O. 14176

20 communication station to relay communications between
said first communication station and said second
communication station.

144. The secure communications system of claim 143 wherein said message for said second communication station is left by said first communication station.

145. The secure communications system of claim 143 wherein said message for said second communication station is left by said central communication station.

146. The secure communications system of claim 143 wherein:

said second communication station
includes a second firewall between said second
5 communication station and said communication medium;
and

10 said second firewall allows only
communication originating at said second station and
prevents communication originating on said
communication medium.

147. The secure communications system of
claim 143 wherein:

 said first communication station is a
premises alarm system; and
5 said second communication station is a
central alarm monitoring station.

148. The secure communications system of claim 143 wherein:

said first communication station is a first premises alarm system; and

5 said second communication station is a
second premises alarm system.

149. The secure communications system of
claim 143 wherein:

 said first communication station is a
premises alarm system; and

5 said second communication station is a
remote communications terminal.

150. The secure communications system of
claim 130 wherein:

 said first communication station is a
premises alarm system; and

5 said second communication station is a
central alarm monitoring station.

151. The secure communications system of
claim 130 wherein:

 said first communication station is a
first premises alarm system; and

5 said second communication station is a
second premises alarm system.

152. The secure communications system of
claim 130 wherein:

 said first communication station is a
premises alarm system; and

5 said second communication station is a
remote communications terminal.

153. The secure communications system of
claim 130 further comprising:

 at said central communication station,
at least one service agent unit for communicating

2025 RELEASE UNDER E.O. 14176

5 between said first communication station and at least
one service on said communications medium; wherein:

at least one of said at least one
service requires a secure identifier for access
thereto; and

10 at least one of said at least one
service agent unit comprises secure identifier storage,
a user at said first communication station registering
said user's secure identifier for said at least one of
said at least one service; whereby:

15 when said user accesses said at least
one of said at least one service, said user need not
transmit said secure identifier over said communication
medium, said secure identifier being transmitted
securely by said service agent unit from said secure
20 identifier storage.

154. A secure communications system for
communicating between first and second communication
stations connected to a communications medium; said
system comprising:

5 a central communication station
connected to said communication medium and having a
secure digital session key generator; wherein:

each of said first and second
communication means further comprises a respective
10 encryption processor for encrypting and decrypting
communications using a digital key;

all communication with said first
communication station is initiated by said first
communication station;

15 all communication with said second
communication station is initiated by said second
communication station;

communication between said first
communication station and said second communication

20 station is established by generating at said secure
digital session key generator a secure digital session
key and leaving a respective message at said central
communication station for each of said first and second
communication stations, each said respective message
25 including said secure digital session key;

when said first communication station
initiates communication with said central communication
station, said first communication station receives said
message including said secure digital session key;

30 when said second communication station
initiates communication with said central communication
station, said second communication station receives
said message including said secure digital session key;
and

35 said first and second communication
stations communicate with one another using said secure
digital session key and said respective encryption
processors.

155. An integrated security and
communications method comprising:

providing a security controller having
at least one sensory input, at least one alarm output
5 and at least one control signal input/output port;

providing a control interface
operatively connected to said at least one control
signal input/output port; and

providing a communications unit
10 connected to a communication channel for providing at
least one communication function, a first communication
port for connection to one of said at least one control
signal input/output port of said security controller
for providing at least one of said at least one
15 communication function to a user at said control
interface, and a second communication port for

connection to a communication device at which said at least one communication function is provided to said user.

156. The method of claim 155 wherein:
said communication channel comprises a telephone line;
said communication device comprises a
5 telephone; and
said at least one communication function comprises telephony.

157. The method of claim 155 wherein:
said communication channel comprises an Internet connection;
said communication device comprises a
5 computer; and
said at least one communication function comprises Internet access.

158. The method of claim 155 further comprising providing at least one function of said control interface at said communication device.

159. A security method for monitoring user premises, said method comprising:
providing at least one sensor;
providing at least one alarm output
5 device;
providing at least one user control interface;
connecting a system controller to said sensor, said output device and said user control
10 interface, said at least one user control interface being used by a user to enter commands affecting a state of a security system;

when said state indicates that said
system is active, monitoring said at least one sensor
15 and outputting an alarm on said alarm output device
when said at least one sensor indicates that an alarm
condition exists; and

connecting a telephone interface unit to
said controller and a telephone line for providing
20 voice mail functionality including one or more of
message retrieval, message waiting indication, and
message header indication; wherein:

said voice mail functionality is
accessible at at least one of said at least one user
25 control interface;

access to said voice mail functionality
is restricted based on said state of said system, said
voice mail functionality being accessible when said
state is consistent with presence of an authorized user
30 on said premises;

said system further having a plurality
of authorized users, and having an authorization unit
at said at least one user control interface for
uniquely identifying each of at least one of said
35 authorized users, wherein:

a particular one of said at least one
authorized user initiates said state consistent with
presence of an authorized user by activating said
authorization unit using an indicium unique to said
40 particular authorized user; and

said telephone interface unit presents
for access, at said user control interface, only voice
mail functions for which said particular authorized
user is authorized.

160. The security method of claim 159 further
comprising:

Approved for Release

providing a keypad at said user control interface; wherein:

5 said indicium comprises a respective passcode unique to each said at least one authorized user; and

 said activating of said authorization unit comprises entering said passcode on said keypad.

161. The security method of claim 159 wherein:

 said authorization unit comprises a receiver at said user control interface;

5 said indicium comprises a respective transmitter uniquely coded to each said at least one authorized user; and

 said activating of said authorization unit comprises actuating said transmitter within
10 communication range of said receiver.

162. The security method of claim 161 wherein said receiver and said coded transmitter are wireless.

163. The security method of claim 159 further comprising:

 providing a token reader at said user control interface; and

5 providing as said indicium a respective coded token unique to each said at least one authorized user; wherein:

 said activating of said authorization unit comprises presenting said token to said token
10 reader.

164. The security method of claim 159 wherein said voice mail functionality is activated automatically upon entry of said system into said state

consistent with presence of an authorized user on said
5 premises.

165. The security method of claim 159 further
comprising remotely controlling, through a remote
access unit which a user remotely controls, during a
single telephone call session to said system from a
5 remote location, both (a) at least one security system
control function, and (b) at least one voice mail
function.

166. The security method of claim 159 wherein
said voice mail functionality comprises playback of an
outgoing message to an incoming caller; said method
further comprising:

5 connecting at least one telephone set to
said telephone line; and

providing a call screening function at
at least one of (a) said at least one telephone set,
and (b) said at least one user control interface, said
10 user control interface including a speaker; wherein:

said call screening function is full-
duplex, allowing said incoming caller to speak an
announcement that is audible at said speaker during
said playback of said outgoing message.

167. The security method of claim 159 further
comprising:

connecting at least one telephone set
connected to said telephone line; and

5 providing an aural indication at said at
least one telephone set when a voice mail message has
been received and is awaiting playback.

168. The security method of claim 159 wherein said user control interface includes a speaker; said method further comprising:

connecting at least one telephone set to
5 said telephone line, said least one telephone set having a ringer;

providing a privacy function whereby said ringer can be deactivated under control of a user; and

10 providing, as part of said privacy function, a privacy breakthrough function whereby a caller issues a command when said privacy function is active for broadcasting a message on said speaker.

169. The security method of claim 159 wherein said voice mail functionality includes a toll saver feature controlled by said state of said system.

170. The security method of claim 169 wherein said toll saver feature is active only when said state of said system indicates absence of authorized users from said premises.

171. The security method of claim 170 further comprising controlling said toll saver feature at said user control interface.

172. The security method of claim 171 further comprising connecting at least one telephone set to said telephone line; wherein:

said toll saver feature can be
5 controlled by a user at at least one of said at least one telephone set.

173. The security method of claim 159 further comprising:

displaying calling party identification data at said user control interface; and

5 responsive to said calling party identification data, generating a distinctive ringing signal different from a standard incoming ringing signal based on said calling party identification data.

174. The security method of claim 173 further comprising generating a first number of distinctive ringing signals, each distinctive ringing signal in said first number of distinctive ringing signals
5 identifying at least one preselected calling party from a second number of preselected calling parties.

175. The security method of claim 174 wherein said first number is equal to said second number, whereby each distinctive ringing signal is associated with a unique preselected calling party.

176. The security method of claim 174 wherein said first number is less than said second number, whereby each distinctive ringing signal is associated with a plurality of said preselected calling parties.

177. The security method of claim 174 wherein said generating of distinctive ringing signals comprises interrupting said standard incoming ringing signal in a second number of ways equal to said second
5 number of distinctive ringing signals, to produce said second number of distinctive ringing signals.

178. The security method of claim 173 wherein said generating of distinctive ringing signals comprises interrupting said standard incoming ringing signal to produce said distinctive ringing signal.

179. The security method of claim 159 further comprising:

displaying calling party identification data at said user control interface;

5 storing instructions for paging a user when said calling party identification data identifies one of at least one particular calling party; and

acting on said instructions and placing a call to a user's pager when said calling party
10 identification data identify one of said at least one particular calling party.

180. The security method of claim 159 further comprising:

connecting at least one telephone set to said telephone line through said telephone interface
5 unit;

providing a speaker at at least one of said at least one user control interface;

providing a public address function at said telephone interface whereby, when a user issues a
10 command at said telephone set:

said telephone set is disconnected from said telephone line and connected to said speaker of said at least one of said at least one user control interface.

181. The security method of claim 180 further comprising connecting said telephone set to said speaker of each said at least one of said at least one user control interface.

182. The security method of claim 180 further comprising, on command of said user, connecting said telephone set to said speaker of any one or more of

11/04/2004 10:43:43 AM

said at least one of said at least one user control
5 interface.

183. The security method of claim 180 further
comprising, when said user issues said command at said
telephone set, maintaining said telephone line in an
off-hook condition while said public address function
5 is in use.

184. The security method of claim 159 further
comprising:

connecting at least one telephone set
connected to said telephone line through said telephone
5 interface unit;

providing a microphone at at least one
of said at least one user control interface;

providing a room monitor function at
said telephone interface unit whereby, when a user
10 issues a command at said telephone set:

said telephone set is disconnected from
said telephone line and connected to said microphone of
said at least one of said at least one user control
interface.

185. The security method of claim 159 further
comprising connecting at least one telephone set to
said telephone line through said telephone interface
unit; wherein:

5 at least one programmable parameter of
said security system is programmable:

(a) at said at least one user control
interface;

(b) at said connected telephone set; and

10 (c) remotely by calling into said system
on said telephone line.

wherein:

5 only a subset of said plurality of
programmable parameters is programmable remotely.

5 at least one programmable parameter of
said security system is programmable; and

responsive to said control signals from said user-controlled processor, disconnecting said telephone interface unit from said telephone line and placing said system in a user-controlled mode.

programming said at least one
5 programmable parameter of said security system;
downloading voice mail messages received
as part of said voice mail functionality from said
telephone interface unit to said user-controlled
processor; and

10 uploading voice prompts composed at said
user-controlled processor to said telephone interface
unit.

189. The security method of claim 187 wherein said user-controlled processor comprises a personal computer.

190. The security method of claim 159 wherein:

said telephone line has central office voice mail associated therewith; and

5 said voice mail functionality comprises indicating a central office voice message waiting.

191. The security method of claim 190 wherein said indicating central office message waiting comprises providing an indication at said user control interface.

192. The security method of claim 191 wherein said providing indication at said user control interface comprises providing visual indication.

193. The security method of claim 191 wherein said providing indication at said user control interface comprises providing aural indication.

194. The security method of claim 190 further comprising connecting at least one telephone set to said telephone line; wherein:

5 said indicating central office message waiting comprises providing an indication at said telephone set.

195. The security method of claim 194 wherein said providing an indication at said telephone set comprises providing an aural indication.

196. The security method of claim 194
wherein:

said telephone set includes a visual
indicator; and

5 said providing an indication at said
telephone set comprises providing a visual indication.

197. The security method of claim 159 wherein
said telephone interface unit further comprises a
remote access unit through which a user controls at
least one security system control function via said
5 telephone line.

198. The security method of claim 197 wherein
said user, through said remote access unit, controls
said at least one security system function from a
telephone at a remote location by calling into said
5 telephone line from said remote location.

199. The security method of claim 197 further
comprising:

connecting at least one telephone set to
said telephone line; wherein:

5 said user, through said telephone
interface unit, controls said at least one security
system function from said telephone set.

200. The security method of claim 159 further
comprising:

connecting at least one telephone set
connected to said telephone line;

5 monitoring said telephone line and, when
an outgoing telephone call is placed on said at least
one telephone set, logging said outgoing telephone
call.

2025 RELEASE UNDER E.O. 14176

201. The security method of claim 200 further comprising:

storing data identifying numbers to which outgoing calls are restricted; and

5 when an outgoing call is placed on said telephone set to one of said numbers to which outgoing calls are restricted, preventing said outgoing call from being completed.

202. The security method of claim 201 further comprising:

further storing at least one user code;

and

5 when said user code is entered during said outgoing call, allowing said outgoing call to be completed to one of said numbers to which outgoing calls are restricted.

203. The security method of claim 159 further comprising connecting said user control interface to an external data network for at least one of (a) sending, and (b) receiving, data.

204. The security method of claim 203 wherein:

said data comprise electronic mail; and access to said electronic mail is

5 restricted based on said state of said system.

205. The security method of claim 204 wherein said electronic mail is accessible when said state is consistent with presence of an authorized user on said premises.

206. The security method of claim 205 wherein said system has a plurality of authorized users; said

FILED 19850300

method further comprising, when a particular authorized user initiates said state consistent with presence of
5 an authorized user by activating said authorization unit:

presenting, for access at said user control interface, only electronic mail addressed to said particular authorized user.

207. The security method of claim 206 further comprising providing a keypad at said user control interface; wherein:

said indicium comprises a passcode
5 unique to said particular authorized user; and
said activation of said authorization unit comprises entry of said passcode at said keypad.

208. The security method of claim 206 wherein:

said authorization unit comprises a receiver; and
5 said indicium comprises a transmitter coded uniquely to said particular authorized user; said method further comprising:
activating said authorization unit by activating said coded transmitter in communication
10 range of said receiver.

209. The security method of claim 206 wherein:

said authorization unit comprises a token reader; and
5 said indicium comprises a token coded uniquely to said particular authorized user; said method further comprising
activating said authorization unit by presenting of said coded token to said reader.


```

                said authorization unit comprises a
receiver;

```

5 said indicium comprises a transmitter
coded uniquely to said one of said at least one
authorized user; said method further comprising:
 activating said authorization unit by
activating said coded transmitter in communication
10 range of said receiver.

217. The security method of claim 214
wherein:

 said authorization unit comprises a
token reader; and
5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; said method further comprising:
 activating said authorization unit by
presenting said coded token to said reader.

218. The security method of claim 203
wherein:

 said external data network is the
Internet;
5 said data comprise World Wide Web pages;
and
 said system has at least one authorized
user; said method further comprising, when one of said
at least one authorized user enters a security system
10 command at said user control interface by activating
said authorization unit:
 retrieving a World Wide Web page
directed to said one of said at least one authorized
user; and
15 displaying said World Wide Web page at
said user control interface.

219. The security method of claim 218 further
comprising:

providing a keypad at said user control interface; wherein:

- 5 said indicium comprises a passcode
unique to said one of said at least one authorized
user; and
 said activation of said authorization
unit comprises entry of said passcode at said keypad.

220. The security method of claim 218
wherein:

- said authorization unit comprises a
receiver; and
5 said indicium comprises a transmitter
coded uniquely to said one of said at least one
authorized user; said method further comprising:
 activating of said authorization unit by
activating said coded transmitter in communication
10 range of said receiver.

221. The security method of claim 220
wherein:

- said transmitter is encoded with
multiple codes; and
5 said activation of said authorization
unit comprises activation of a selected one of said
multiple codes by said one of said at least one
authorized user; said method further comprising:
 retrieving a different World Wide Web
10 page based on which of said multiple codes has been
selected.

222. The security method of claim 218
wherein:

- said authorization unit comprises a
token reader; and

5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; said method further comprising:
 activating said authorization unit by
presenting said coded token to said reader.

223. The security method of claim 203
wherein:

 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface by activating said authorization unit; and
 said external data network is the
Internet; said method further comprising, on activation
10 of said authorization unit by said one of said at least
one authorized user:
 logging said one of said at least one
authorized user onto the Internet at said user control
interface.

224. The security method of claim 203
wherein:

 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface by activating said authorization unit using
an indicium unique to said one of said at least one
authorized user;
10 said one of said at least one user uses
said external data network to access a financial
institution to perform a financial transaction; and
 said indicium is registered with said
financial institution as an identifier of said one of

2025 RELEASE UNDER E.O. 14176

15 said at least one authorized user; said method further comprising:

 sending said indicium to said financial institution as part of said financial transaction.

225. The security method of claim 203 further comprising:

 transmitting security data signals to a central communication station via said external data
5 network and an alternate channel and awaiting acknowledgment thereof; and

 when said acknowledgment arrives from a first one of said external data network and said alternate channel, terminating transmission of said
10 security data on a second one of said external data network and said alternate channel.

226. The security method of claim 225 wherein:

 one of said external data network and said alternate channel normally operates faster than
5 another of said external data network and said alternate channel; and

 transmitting of said security data signals to said central communication station via said one of said external data network and said alternate
10 channel begins before transmitting of said security data signals to said central communication station via said another of said external data network and said alternate channel.

227. The security method of claim 225 further comprising:

 providing a firewall between said user control interface and said external data network, said
5 firewall allowing only communication originating at

FILED "1980888"

said system and prevents communication originating on said external data network; and

10 to receive said acknowledgment from said central communication station, initiating communication with said external data network so that said firewall allows said communication, said initiated communication including a query to said external data network for said acknowledgment to be communicated from said central communication station to said system.

228. The security method of claim 227 wherein said query to said external network comprises a query to said central communication station.

229. The security method of claim 225 wherein said alternate channel is said telephone line.

230. The security method of claim 203 further comprising:

5 transmitting security data signals to a central communication station via a plurality of channels; and

when said acknowledgment arrives from a first one of said plurality of channels, terminating transmission of said security data on each other one of said plurality of channels.

231. The security method of claim 230 wherein:

5 one of said plurality of channels normally operates faster than others of said plurality of channels; and

transmitting of said security data signals to said central communication station via said one of said plurality of channels begins before transmitting of said security data signals to said

TOP SECRET

- 10 central communication station via said others of said plurality of channels.

232. The security method of claim 203 further comprising accepting commands from a user via said external data network.

233. The security method of claim 232 further comprising:

- providing a firewall between said user control interface and said external data network, said
5 firewall allowing only communication originating at said system and preventing communication originating on said external data network; and

- to receive said commands from said user, initiating communication with said external data
10 network so that said firewall allows said communication, said initiated communication including a query to said external data network for commands issued by said user to be communicated from said external data network to said system.

234. The security method of claim 203 further comprising sending security data signals to predetermined recipients via said external data network.

235. The security method of claim 203 further comprising providing more than one of said user control interface, each said user control interface functioning as an independent terminal of said external data
5 network.

236. The security method of claim 203 further comprising:

providing a firewall between said user control interface and said external data network, said
5 firewall allowing only communication originating at said system and preventing communication originating on said external data network; and
to receive data, initiating communication with said external data network so that
10 said firewall allows said communication, said initiated communication including a query to said external data network for data sought to be communicated from said external data network to said system.

237. A security method for monitoring user premises, said method comprising:
providing at least one sensor;
providing at least one alarm output
5 device;
providing at least one user control interface;
providing a system controller connected to said sensor, said output device and said user
10 control interface; wherein:
at least one of said at least one user control interface is connected to an external data network for at least one of (a) sending, and (b) receiving, data.

238. The security method of claim 237 wherein said data comprise electronic mail.

239. The security method of claim 237 wherein:
said at least one user control interface is used by a user to enter commands affecting a state
5 of said system; said method further comprising:

when said state indicates that said system is active, monitoring said at least one sensor and outputting an alarm on said alarm output device when said at least one sensor indicates that an alarm
10 condition exists.

240. The security method of claim 239 wherein:

said data comprise electronic mail; and
access to said electronic mail is
5 restricted based on said state of said system.

241. The security method of claim 240 wherein said electronic mail is accessible when said state is consistent with presence of an authorized user on said premises.

242. The security method of claim 241 wherein:

there are a plurality of authorized users, said system having an authorization unit for
5 uniquely identifying each of at least one of said authorized users; and

a particular authorized user initiates said state consistent with presence of an authorized user by activating said authorization unit using an
10 indicium unique to said particular authorized user; said method further comprising:

presenting, for access at said user control interface, only electronic mail addressed to said particular authorized user.

243. The security method of claim 242 further comprising:

providing a keypad at said user control interface; wherein:

5 said indicium comprises a respective
passcode unique to each said at least one authorized
user; and

 said activating of said authorization
unit comprises entry of said passcode at said keypad.

244. The security method of claim 242
wherein:

 said user control interface comprises a
receiver; and

5 said indicium comprises a respective
transmitter uniquely coded to each of said at least one
authorized user; said method further comprising:

 activating said authorization unit by
activating said coded transmitter in communication
10 range of said receiver.

245. The security method of claim 242
wherein:

 said user control interface comprises a
token reader; and

5 said indicium comprises a token uniquely
coded to each of said at least one authorized user;
said method further comprising:

 activating said authorization unit by
presenting said coded token to said reader.

246. The security method of claim 241
wherein:

 said system has a plurality of
authorized users, and has an authorization unit for
5 uniquely identifying each of at least one of said
authorized users; and

 a particular authorized user initiates
said state consistent with presence of an authorized
user by activating said authorization unit using an

10 indicium unique to said particular authorized user;
said method further comprising:

presenting access at said user control
interface to electronic mail message sending from said
particular authorized user.

247. The security method of claim 246 further
comprising:

providing a keypad at said user control
interface; wherein:

5 said indicium comprises a respective
passcode unique to each of said at least one authorized
user; and

said activation of said authorization
unit indicium comprises entry of said passcode at said
10 keypad.

248. The security method of claim 246 further
comprising:

providing a receiver at said user
control interface; wherein:

5 said indicium comprises a respective
transmitter uniquely coded to each of said at least one
authorized user; and

said activation of said authorization
unit comprises activation of said coded transmitter in
10 communication range of said receiver.

249. The security method of claim 246
wherein:

said user control interface comprises a
token reader; and

5 said indicium comprises a respective
token uniquely coded to each of said at least one
authorized user; said method further comprising:

activating said authorization unit by presenting said coded token to said reader.

250. The security method of claim 237 wherein:

said data comprise electronic mail; and
said system has at least one authorized
5 user, and has an authorization unit for uniquely
identifying each of at least one of said authorized
users; said method further comprising, when one of said
at least one authorized user enters a security system
command at said user control interface by activating
10 said authorization unit using an indicium unique to
said one of said at least one authorized user:

sending an electronic mail message to a
predetermined recipient advising of said entry of said
command by said user.

251. The security method of claim 250 further comprising:

providing a keypad at said user control
interface; wherein:

5 said indicium comprises a respective
passcode unique to each of said at least one authorized
user; and

said activation of said authorization
unit comprises entry of said passcode at said keypad.

252. The security method of claim 250 wherein:

said user control interface comprises a
receiver; and

5 said indicium comprises a respective
transmitter uniquely coded for each of said at least
one authorized user; said method further comprising:

activating said authorization unit by
activating said coded transmitter in communication
10 range of said receiver.

253. The security method of claim 250
wherein:

said user control interface comprises a
token reader; and

5 said indicium comprises a token uniquely
coded to each of said at least one authorized user;
said method further comprising:

activating said authorization unit by
presenting said coded token to said reader.

254. The security method of claim 237
wherein:

said external data network is the
Internet;

5 said data comprise World Wide Web pages;
said system has at least one authorized
user, and has an authorization unit for uniquely
identifying each of at least one of said authorized
users; said method further comprising, when one of said
10 at least one authorized user enters a security system
command at said user control interface by activating
said authorization unit using an indicium unique to
said one of said at least one authorized user:

retrieving a World Wide Web page
15 directed to said one of said at least one authorized
user and displaying said World Wide Web page at said
user control interface.

255. The security method of claim 254 further
comprising:

providing a keypad at said user control
interface; wherein:

5 said indicium comprises a respective
passcode unique to each of said at least one authorized
user; and

 said activation of said authorization
unit comprises entry of said passcode at said keypad.

256. The security method of claim 254
wherein:

 said user control interface comprises a
receiver; and

5 said indicium comprises a respective
transmitter uniquely coded for each of said at least
one authorized user; said method further comprising:
 activating said authorization unit by
activating said coded transmitter in communication
10 range of said receiver.

257. The security method of claim 256
wherein:

 said respective transmitter is encoded
with multiple codes; and

5 said activation of said authorization
unit comprises activation of a selected one of said
multiple codes by said one of said at least one
authorized user; said method further comprising:
 retrieving a different World Wide Web
10 page based on which of said multiple codes has been
selected.

258. The security method of claim 254
wherein:

 said user control interface comprises a
token reader; and

5 said indicium comprises a respective
token uniquely coded for each of said at least one
authorized user; said method further comprising:

said at least one authorized user; said method further comprising:

20 sending said indicium to said financial institution as part of said financial transaction.

261. The security method of claim 237 further comprising:

5 transmitting security data signals to a central communication station via said external data network and an alternate channel and awaiting acknowledgment thereof; and

10 when said acknowledgment arrives from a first one of said external data network and said alternate channel, terminating transmission of said security data on a second one of said external data network and said alternate channel.

262. The security method of claim 261 wherein:

5 one of said external data network and said alternate channel normally operates faster than another of said external data network and said alternate channel; and

10 transmitting of said security data signals to said central communication station via said one of said external data network and said alternate channel begins before transmitting of said security data signals to said central communication station via said another of said external data network and said alternate channel.

263. The security method of claim 261 wherein:

5 there is a firewall between said user control interface and said external data network, said firewall allowing only communication originating at

2025 RELEASE UNDER E.O. 14176

said system and preventing communication originating on said external data network; said method further comprising:

- to receive said acknowledgment from said
- 10 central communication station, initiating communication with said external data network so that said firewall allows said communication, said initiated communication including a query to said external data network for said acknowledgment to be communicated from said
- 15 central communication station to said system.

264. The security method of claim 263 wherein said query to said external network comprises a query to said central communication station.

265. The security method of claim 261 wherein said alternate channel is said telephone line.

266. The security method of claim 237 further comprising:

- transmitting security data signals to a central communication station via a plurality of
- 5 channels; and

when said acknowledgment arrives from a first one of said plurality of channels, terminating transmission of said security data on each other one of said plurality of channels.

267. The security method of claim 266 wherein:

- one of said plurality of channels normally operates faster than others of said plurality
- 5 of channels; and

transmitting of said security data signals to said central communication station via said one of said plurality of channels begins before

444-433000

transmitting of said security data signals to said
10 central communication station via said others of said
plurality of channels.

268. The security method of claim 237 further
comprising accepting commands from a user via said
external data network.

269. The security method of claim 268
wherein:

there is a firewall between said user
control interface and said external data network, said
5 firewall allowing only communication originating at
said system and preventing communication originating on
said external data network; said method further
comprising:

to receive said commands from said user,
10 initiating communication with said external data
network so that said firewall allows said
communication, said initiated communication including a
query to said external data network for commands issued
by said user to be communicated from said external data
15 network to said system.

270. The security method of claim 237 further
comprising sending security data signals to
predetermined recipients via said external data
network.

271. The security method of claim 237
wherein:

there is a firewall between said user
control interface and said external data network, said
5 firewall allowing only communication originating at
said system and preventing communication originating on

FILED 435000

said external data network; said method further comprising:

- to receive data, initiating
- 10 communication with said external data network so that said firewall allows said communication, said initiated communication including a query to said external data network for data sought to be communicated from said external data network to said system.

272. A secure communications method for communicating between first and second communication stations connected to a communications medium; said method comprising:

- 5 providing a central communication station connected to said communication medium;
- initiating all communication between said first communication station and said central communication station at said first communication
- 10 station;
- establishing communication between said first communication station and said second communication station by leaving a message for said first communication station at said central
- 15 communication station indicating communication is desired between said first communication station and said second communication station; and
- when said first communication station initiates communication with said central communication
- 20 station, said first communication station receiving said message for said first communication station, maintaining its initiated communication with said central communication station and instructing said central communication station to relay communications
- 25 between said first communication station and said second communication station.

273. The secure communications method of claim 272 further comprising said second communication station leaving said message for said first communication station.

274. The secure communications method of claim 272 further comprising said central communication station leaving said message for said first communication station.

275. The secure communications method of claim 272 wherein said first communication station includes a first firewall between said first communication station and said communication medium,
5 said first firewall allowing only communication originating at said first station and preventing communication originating on said communication medium.

276. The secure communications method of claim 272 further comprising:

at said central communication station and said first communication station, storing a first
5 digital key and associating said stored first digital key with said first communication station;

at said first communication station, encrypting each communication sent to said central communication station, and decrypting each
10 communication received from said central communication station, using said first digital key identified with said first communication station; and

at said central communication station, encrypting with said first station digital key each
15 communication sent to said first communication station and decrypting with said first station digital key each communication received from said first communication station.

FOI b7D 49630300

277. The secure communications method of claim 276 further comprising:

initiating all communication between said second communication station and said central communication station at said second communication station;

establishing communication between said second communication station and said first communication station by leaving a message for said second communication station at said central communication station indicating communication is desired between said second communication station and said first communication station; and

when said second communication station initiates communication with said central communication station, said second communication station receiving said message for said second communication station, maintaining its initiated communication with said central communication station and instructing said central communication station to relay communications between said second communication station and said first communication station.

278. The secure communications method of claim 277 further comprising said first communication station leaving said message for said second communication station.

279. The secure communications method of claim 277 further comprising said central communication station leaving said message for said second communication station.

280. The secure communications method of claim 277 wherein said second communication station

2025 RELEASE UNDER E.O. 14176

includes a second firewall between said second
communication station and said communication medium,
5 said second firewall allowing only communication
originating at said second station and preventing
communication originating on said communication medium.

281. The secure communications method of
claim 277 wherein:

at said central communication station
and said second communication station, storing a second
5 digital key and associating said stored second digital
key with said second communication station;

at said second communication station,
encrypting each communication sent to said central
communication station, and decrypting each
10 communication received from said central communication
station, using said second digital key identified with
said second communication station; and

at said central communication station,
encrypting with said second station digital key each
15 communication sent to said second communication station
and decrypting with said second station digital key
each communication received from said second
communication station.

282. The secure communications method of
claim 272 further comprising:

initiating all communication between
said second communication station and said central
5 communication station at said second communication
station;

establishing communication between said
second communication station and said first
communication station by leaving a message for said
10 second communication station at said central
communication station indicating communication is

desired between said second communication station and said first communication station; and

when said second communication station
15 initiates communication with said central communication station, said second communication station receiving said message for said second communication station, maintaining its initiated communication with said central communication station and instructing said
20 central communication station to relay communications between said second communication station and said first communication station.

283. The secure communications method of claim 282 further comprising said first communication station leaving said message for said second communication station.

284. The secure communications method of claim 282 further comprising said central communication station leaving said message for said second communication station.

285. The secure communication method of claim 282 wherein said second communication station includes a second firewall between said second communication station and said communication medium,
5 said second firewall allowing only communication originating at said second station and preventing communication originating on said communication medium.

286. The secure communications method of claim 272 further comprising:

at said central communication station,
providing at least one service agent unit for
5 communicating between said first communication station

2025 RELEASE UNDER E.O. 14176

and at least one service on said communications medium;
wherein:

- at least one of said at least one
service requires a secure identifier for access
10 thereto; said method further comprising:
providing secure storage at at least one
of said at least one service agent unit, and storing in
said secure storage a secure identifier for said at
least one of said at least one service registered at
15 said secure storage by a user at said first
communication station; whereby:
when said user accesses said at least
one of said at least one service, said user need not
transmit said secure identifier over said communication
20 medium, said secure identifier being transmitted
securely by said service agent unit from said secure
identifier storage.

287. A secure communications method for
communicating between first and second communication
stations connected to a communications medium; said
method comprising:

- 5 providing a central communication
station connected to said communication medium and
having a secure digital session key generator;
providing at each of said first and
second communication means a respective encryption
10 processor for encrypting and decrypting communications
using a digital key;
initiating all communication with said
first communication station at said first communication
station;
15 initiating all communication with said
second communication station at said second
communication station;

establishing communication between said
first communication station and said second
20 communication station by generating at said secure
digital session key generator a secure digital session
key and leaving a respective message at said central
communication station for each of said first and second
communication stations, each said respective message
25 including said secure digital session key;
when said first communication station
initiates communication with said central communication
station, said first communication station receiving
said message including said secure digital session key;
30 when said second communication station
initiates communication with said central communication
station, said second communication station receiving
said message including said secure digital session key;
and
35 said first and second communication
stations communicating with one another using said
secure digital session key and said respective
encryption processors.

288. An integrated security and
communications system comprising:

a security controller means having at
least one means for accepting sensory input, at least
5 one means for outputting an alarm and at least one
means for inputting/outputting a control signal;

a control interface means operatively
connected to said at least one means for inputting/
outputting a control signal; and

10 means for communicating connected to a
communication channel for providing at least one
communication function, a first communication port for
connection to one of said at least one means of said
security controller for inputting/outputting a control

15 signal for providing at least one of said at least one
communication function to a user at said control
interface means, and a second communication port for
connection to a communication device at which said at
least one communication function is provided to said
20 user.

289. The system of claim 288 wherein:
said communication channel comprises a
telephone line; and
said communication device comprises a
5 telephone.

290. The system of claim 289 wherein said at
least one communication function comprises telephony.

291. The system of claim 288 wherein:
said communication channel comprises an
Internet connection;
said means for communicating comprises
5 means for computing; and
said at least one communication function
comprises Internet access.

292. The system of claim 288 wherein said
means for communicating provides at least one function
of said control interface at said communication device.

293. A security system for monitoring user
premises, said system comprising:
at least one means for sensing;
at least one means for outputting an
5 alarm;
at least one user control interface
means;

4935060

10

20

25

30

35

40

for access, at said user control interface means, only

voice mail functions for which said particular
45 authorized user is authorized.

294. The security system of claim 293
wherein:

said means for authorizing comprises
keypad means at said user control interface means;

5 said indicium comprises a respective
passcode unique to each said at least one authorized
user; and

said activating of said means for
authorizing comprises entering said passcode on said
10 keypad means.

295. The security system of claim 293
wherein:

said means for authorizing comprises
means for receiving at said user control interface
5 means;

said indicium comprises a respective
means for transmitting uniquely coded to each said at
least one authorized user; and

said activating of said means for
10 authorizing comprises actuating said means for
transmitting within communication range of said means
for receiving.

296. The security system of claim 295 wherein
said means for receiving and said coded means for
transmitting are wireless.

297. The security system of claim 293
wherein:

said means for authorizing comprises
means for reading a token at said user control
5 interface means;

said indicium comprises a respective coded token unique to each said at least one authorized user; and

said activating of said means for
10 authorizing comprises presenting said token to said token reading means.

298. The security system of claim 293 wherein said voice mail functionality is activated automatically upon entry of said system into said state consistent with presence of an authorized user on said
5 premises.

299. The security system of claim 293 wherein said telephone interface means further comprises means for remote access through which a user remotely controls, during a single telephone call session to
5 said system from a remote location, both (a) at least one security system control function, and (b) at least one voice mail function.

300. The security system of claim 293 further comprising at least one telephone set connected to said telephone line; wherein:

said voice mail functionality comprises
5 playback of an outgoing message to an incoming caller;
said telephone interface means further provides a call screening function at at least one of (a) said at least one telephone set, and (b) said at least one user control interface means, said user
10 control interface means including speaker means; and
said call screening function is full-duplex, allowing said incoming caller to speak an announcement that is audible at said speaker means during said playback of said outgoing message.

301. The security system of claim 293 further comprising at least one telephone set connected to said telephone line; wherein:

- 5 said telephone interface means further provides an aural indication at said at least one telephone set when a voice mail message has been received and is awaiting playback.

302. The security system of claim 293 further comprising at least one telephone set connected to said telephone line, said least one telephone set having means for ringing; wherein:

- 5 said user control interface means includes speaker means; and
 said telephone interface means further provides:
 a privacy function whereby said means
10 for ringing can be deactivated under control of a user, and
 as part of said privacy function, a privacy breakthrough function whereby a caller issues a command when said privacy function is active for
15 broadcasting a message on said speaker means.

303. The security system of claim 293 wherein said voice mail functionality includes a toll saver feature controlled by said state of said system.

304. The security system of claim 303 wherein said toll saver feature is active only when said state of said system indicates absence of authorized users from said premises.

305. The security system of claim 304 wherein said toll saver feature can further be controlled by a user at said user control interface means.

19950604

306. The security system of claim 305 further comprising at least one telephone set connected to said telephone line; wherein:

5 said toll saver feature can be controlled by a user at at least one of said at least one telephone set.

307. The security system of claim 293 wherein said telephone interface means further comprises:

5 means for displaying calling party identification data, said calling party identification data being displayed at said user control interface means; and

10 means responsive to said calling party identification data for generating a distinctive ringing signal, different from a standard incoming ringing signal, based on said calling party identification data.

308. The security system of claim 307 wherein said means for generating a distinctive ringing signal generates a first number of distinctive ringing signals, each distinctive ringing signal in said first number of distinctive ringing signals identifying at least one preselected calling party from a second number of preselected calling parties.

309. The security system of claim 308 wherein said first number is equal to said second number, whereby each distinctive ringing signal is associated with a unique preselected calling party.

310. The security system of claim 308 wherein said first number is less than said second number,

whereby each distinctive ringing signal is associated with a plurality of said preselected calling parties.

311. The security system of claim 308 wherein said means for generating distinctive ringing signals comprises means for interrupting said standard incoming ringing signal in a second number of ways equal to said
5 second number of distinctive ringing signals, to produce said second number of distinctive ringing signals.

312. The security system of claim 307 wherein said means for generating distinctive ringing signals comprises means for interrupting said standard incoming ringing signal to produce said distinctive ringing
5 signal.

313. The security system of claim 293 wherein said telephone interface means further comprises:
means for displaying calling party identification data at said user control interface;
5 means for storing instructions for paging a user when said calling party identification data identifies one of at least one particular calling party; and
processor means for acting on said
10 instructions and placing a call to a user's pager when said calling party identification data identify one of said at least one particular calling party.

314. The security system of claim 293 further comprising at least one telephone set connected to said telephone line through said telephone interface means; wherein:
5 at least one of said at least one user control interface means comprises speaker means;

said telephone interface means further comprises a public address function; whereby, when a user issues a command at said telephone set:

10 said telephone set is disconnected from said telephone line and connected to said speaker means of said at least one of said at least one user control interface means.

315. The security system of claim 314 wherein said telephone set is connected to said speaker means of each said at least one of said at least one user control interface means.

316. The security system of claim 314 wherein, on command of said user, said telephone set is connected to said speaker means of any one or more of said at least one of said at least one user control
5 interface means.

317. The security system of claim 314 wherein, when said user issues said command at said telephone set, said telephone interface means maintains said telephone line in an off-hook condition while said
5 public address function is in use.

318. The security system of claim 293 further comprising at least one telephone set connected to said telephone line through said telephone interface means; wherein:

5 at least one of said at least one user control interface means comprises a microphone;

 said telephone interface means further comprises a room monitor function; whereby, when a user issues a command at said telephone set:

10 said telephone set is disconnected from said telephone line and connected to said microphone of

said at least one of said at least one user control interface means.

319. The security system of claim 293 further comprising at least one telephone set connected to said telephone line through said telephone interface means; wherein:

5 at least one programmable parameter of said security system is programmable:

 (a) at said at least one user control interface means;

 (b) at said connected telephone set; and

10 (c) remotely by calling into said system on said telephone line.

320. The security system of claim 319 wherein:

 there are a plurality of said programmable parameters; and

5 only a subset of said plurality of programmable parameters is programmable remotely.

321. The security system of claim 293 further comprising at least one user-controlled processor means connected via modem means to said telephone line through said telephone interface means; wherein:

5 at least one programmable parameter of said security system is programmable;

 said telephone interface means includes means for detecting control signals sent from said user-controlled processor means through said modem
10 means; whereby:

 responsive to said control signals from said user-controlled processor means, said telephone interface means disconnects from said telephone line and enters a user-controlled mode.

322. The security system of claim 321 wherein in said user-controlled mode said user-controlled processor means performs any one of:

- programming said at least one
- 5 programmable parameter of said security system;
- downloading voice mail messages received as part of said voice mail functionality from said telephone interface means to said user-controlled processor means; and
- 10 uploading voice prompts composed at said user-controlled processor means to said telephone interface means.

323. The security system of claim 321 wherein said user-controlled processor means comprises a personal computer.

324. The security system of claim 293 wherein:

- said telephone line has central office voice mail associated therewith; and
- 5 said voice mail functionality comprises indicating a central office voice message waiting.

325. The security system of claim 324 wherein said indicating central office message waiting comprises providing an indication at said user control interface.

326. The security system of claim 325 wherein said indication at said user control interface is visual.

327. The security system of claim 325 wherein said indication at said user control interface is aural.

328. The security system of claim 324 further comprising at least one telephone set connected to said telephone line; wherein:

said indicating central office message
5 waiting comprises providing an indication at said telephone set.

329. The security system of claim 328 wherein said indication at said telephone set is aural.

330. The security system of claim 328 wherein:

said telephone set includes means for
indicating visually; and
5 said indication at said telephone set is
visual.

331. The security system of claim 293 wherein said telephone interface means further comprises means for remote access through which a user controls at least one security system control function via said
5 telephone line.

332. The security system of claim 331 wherein said user, through said means for remote access, controls said at least one security system function from a telephone at a remote location by calling into
5 said telephone line from said remote location.

333. The security system of claim 331 further comprising at least one telephone set connected to said telephone line; wherein:

said user, through said telephone
5 interface means, controls said at least one security
system function from said telephone set.

334. The security system of claim 293 further
comprising at least one telephone set connected to said
telephone line; wherein:

said telephone interface means monitors
5 said telephone line and, when an outgoing telephone
call is placed on said at least one telephone set, logs
said outgoing telephone call.

335. The security system of claim 334
wherein:

said telephone interface means comprises
means for storing data identifying numbers to which
5 outgoing calls are restricted; and

when an outgoing call is placed on said
telephone set to one of said numbers to which outgoing
calls are restricted, said telephone interface means
prevents said outgoing call from being completed.

336. The security system of claim 335
wherein:

said means for storing further stores at
least one user code; and
5 when said user code is entered during
said outgoing call, said telephone interface means
allows said outgoing call to be completed to one of
said numbers to which outgoing calls are restricted.

337. The security system of claim 293 wherein
said user control interface is connected to an external
data network for at least one of (a) sending, and
(b) receiving, data.

338. The security system of claim 337
wherein:

said data comprise electronic mail; and
access to said electronic mail is
5 restricted based on said state of said system.

339. The security system of claim 338 wherein
said electronic mail is accessible when said state is
consistent with presence of an authorized user on said
premises.

340. The security system of claim 339 having
a plurality of authorized users, wherein:

when a particular authorized user
initiates said state consistent with presence of an
5 authorized user by activating said means for
authorizing, said user control interface means
presents, for access at said user control interface
means, only electronic mail addressed to said
particular authorized user.

341. The security system of claim 340
wherein:

said means for authorizing comprises
keypad means at said user control interface means;
5 said indicium comprises a passcode
unique to said particular authorized user; and
said activation of said means for
authorizing comprises entry of said passcode at said
keypad means.

342. The security system of claim 340
wherein:

said means for authorizing comprises
means for receiving;

5 said indicium comprises means for
transmitting coded uniquely to said particular
authorized user; and

 said activation of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

343. The security system of claim 342 wherein
said means for receiving and said coded means for
transmitting are wireless.

344. The security system of claim 340
wherein:

 said means for authorizing comprises
means for reading a token;

5 said indicium comprises a token coded
uniquely to said particular authorized user; and

 said activation of said means for
authorizing unit comprises presentation of said coded
token to said token reading means.

345. The security system of claim 339 having
a plurality of authorized users, wherein:

 when a particular authorized user
initiates said state consistent with presence of an
5 authorized user by activating said means for
authorizing using an indicium unique to said particular
authorized user, said user control interface means
presents access, at said user control interface means,
to electronic mail message sending from said particular
10 authorized user.

346. The security system of claim 345
wherein:

said means for authorizing comprises
keypad means at said user control interface means;
5 said indicium comprises a passcode
unique to said particular authorized user; and
 said presentation of said indicium
comprises entry of said passcode at said keypad means.

347. The security system of claim 345
wherein:

 said means for authorizing comprises
means for receiving;
5 said indicium comprises means for
transmitting coded uniquely to said particular
authorized user; and
 said activation of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

348. The security system of claim 347 wherein
said means for receiving and said coded means for
transmitting are wireless.

349. The security system of claim 345
wherein:

 said means for authorizing comprises
means for reading a token;
5 said indicium comprises a token coded
uniquely to said particular authorized user; and
 said activation of said means for
authorizing comprises presentation of said coded token
to said means for reading.

350. The security system of claim 337
wherein:

 said data comprise electronic mail;

FILED OCT 19 1990

said system has at least one authorized
5 user; and

when one of said at least one authorized
user enters a security system command at said user
control interface by activating said means for
authorizing, said user control interface means sends an
10 electronic mail message to a predetermined recipient
advising of said entry of said command by said one of
said at least one authorized user.

351. The security system of claim 350
wherein:

said means for authorizing comprises
keypad means at said user control interface means;
5 said indicium comprises a passcode
unique to said one of said at least one authorized
user; and

said activation of said means for
authorizing comprises entry of said passcode at said
10 keypad means.

352. The security system of claim 350
wherein:

said means for authorizing comprises
means for receiving;
5 said indicium comprises means for
transmitting coded uniquely to said one of said at
least one authorized user; and

said activation of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

353. The security system of claim 352 wherein
said means for receiving and said coded means for
transmitting are wireless.

354. The security system of claim 350

wherein:

said means for authorizing comprises
means for reading a token;

5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; and

said activation of said means for
authorizing comprises presentation of said coded token
10 to said means for reading.

355. The security system of claim 337

wherein:

said external data network is the
Internet;

5 said data comprise World Wide Web pages;
said system has at least one authorized
user; and

when one of said at least one authorized
user enters a security system command at said user
10 control interface means by activating said means for
authorizing, said system retrieves a World Wide Web
page directed to said one of said at least one
authorized user and displays said World Wide Web page
at said user control interface means.

356. The security system of claim 355

wherein:

said means for authorizing comprises
keypad means;

5 said indicium comprises a passcode
unique to said one of said at least one authorized
user; and

FILED IN 435033

said activation of said means for
authorizing comprises entry of said passcode at said
10 keypad means.

357. The security system of claim 355
wherein:

said means for authorizing comprises
means for receiving;

5 said indicium comprises means for
transmitting coded uniquely to said one of said at
least one authorized user; and

said activation of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

358. The security system of claim 357 wherein
said means for receiving and said coded means for
transmitting are wireless.

359. The security system of claim 357
wherein:

said means for transmitting is encoded
with multiple codes;

5 said activation of said means for
authorizing comprises activation of a selected one of
said multiple codes by said one of said at least one
authorized user; and

said system retrieves a different World
10 Wide Web page based on which of said multiple codes has
been selected.

360. The security system of claim 355
wherein:

said means for authorizing comprises
means for reading a token;

5 said indicium comprises a token coded
uniquely to said one of said at least one authorized
user; and

 said activation of said means for
authorizing comprises presentation of said coded token
10 to said means for reading.

361. The security system of claim 337
wherein:

 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface means by activating said means for
authorizing;

 said external data network is the
10 Internet; and

 said activation of said means for
authorizing logs said one of said at least one
authorized user onto the Internet at said user control
interface means.

362. The security system of claim 337
wherein:

 said system has at least one authorized
user;

5 one of said at least one authorized user
enters a security system command at said user control
interface means by activating said means for
authorizing using an indicium unique to said one of
said at least one authorized user;

10 said one of said at least one authorized
user uses said external data network to access a
financial institution to perform a financial
transaction;

15 said indicium is registered with said
financial institution as an identifier of said one of
said at least one authorized user; and

 said indicium is sent to said financial
institution as part of said financial transaction.

363. The security system of claim 337 wherein
functions of said system are remotely accessible via
said external data network.

364. The security system of claim 337
wherein:

 said system transmits security data
signals to a central communication station via said
5 external data network and an alternate channel and
awaits acknowledgment thereof; and

 when said acknowledgment arrives from a
first one of said external data network and said
alternate channel, said system terminates transmission
10 of said security data on a second one of said external
data network and said alternate channel.

365. The security system of claim 364
wherein:

 one of said external data network and
said alternate channel normally operates faster than
5 another of said external data network and said
alternate channel; and

 said system begins transmission of said
security data signals on said one of said external data
network and said alternate channel before beginning
10 transmission of said security data signals on said
another of said external data network and said
alternate channel.

5 said firewall means allows only
communication originating at said system and prevents
communication originating on said external data
network; and

to receive said acknowledgment from said
10 central communication station, said system initiates
communication with said external data network so that
said firewall means allows said communication, said
initiated communication including a query to said
external data network for said acknowledgment to be
15 communicated from said central communication station to
said system.

367. The security system of claim 366 wherein said query to said external network comprises a query to said central communication station.

368. The security system of claim 364 wherein said alternate channel is said telephone line.

369. The security system of claim 337
wherein:

said system transmits security data signals to a central communication station via a plurality of channels; and

when said acknowledgment arrives from a first one of said plurality of channels, said system terminates transmission of said security data on each other one of said plurality of channels.

370. The security system of claim 369
wherein:

5 of channels; and

10 channels.

external data network.

interface and said external data network; wherein:

5 communication originating at said system and prevents
communication originating on said external data
network; and

10 data network so that said firewall means allows said communication, said initiated communication including a query to said external data network for commands issued by said user to be communicated from said external data network to said system.

network.

means, each said user control interface means

functioning as an independent terminal of said external
5 data network.

375. The security system of claim 337 further
comprising firewall means between said user control
interface means and said external data network;
wherein:

5 said firewall means allows only
communication originating at said system and prevents
communication originating on said external data
network; and
 to receive data, said system initiates
10 communication with said external data network so that
said firewall means allows said communication, said
initiated communication including a query to said
external data network for data sought to be
communicated from said external data network to said
15 system.

376. A security system for monitoring user
premises, said system comprising:

 at least one means for sensing;
 at least one means for outputting an
5 alarm;
 at least one user control interface
means; and
 a system controller means connected to
said means for sensing, said means for outputting an
10 alarm and said user control interface means; wherein:
 at least one of said at least one user
control interface means is connected to an external
data network for at least one of (a) sending, and
(b) receiving, data.

377. The security system of claim 376 wherein
said data comprise electronic mail.

FOUO 49530000

378. The security system of claim 376
wherein:

said at least one user control interface
means is used by a user to enter commands affecting a
5 state of said system; and

said system, when said state indicates
that said system is active, monitors said at least one
means for sensing and outputs an alarm on said means
for outputting an alarm when said at least one means
10 for sensing indicates that an alarm condition exists.

379. The security system of claim 378
wherein:

said data comprise electronic mail; and
access to said electronic mail is
restricted based on said state of said system.

380. The security system of claim 379 wherein
said electronic mail is accessible when said state is
consistent with presence of an authorized user on said
premises.

381. The security system of claim 380 having
a plurality of authorized users, and having means for
authorizing for uniquely identifying each of at least
one of said authorized users, wherein:

5 a particular authorized user initiates
said state consistent with presence of an authorized
user by activating said authorization unit using an
indicium unique to said particular authorized user; and
said user control interface means
10 presents for access at said user control interface
means only electronic mail addressed to said particular
authorized user.

382. The security system of claim 381
wherein:

said user control interface means
comprises keypad means;

5 said indicium comprises a respective
passcode unique to each said at least one authorized
user; and

 said activating of said means for
authorizing comprises entry of said passcode at said
10 keypad means.

383. The security system of claim 381
wherein:

said user control interface means
comprises means for receiving;

5 said indicium comprises a respective
means for transmitting uniquely coded to each of said
at least one authorized user; and

 said activating of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

384. The security system of claim 383 wherein
said means for receiving and said coded means for
transmitting are wireless.

385. The security system of claim 381
wherein:

said user control interface means
comprises means for reading a token;

5 said indicium comprises a token uniquely
coded to each of said at least one authorized user; and

 said activating of said means for
authorizing comprises presentation of said coded token
to said means for reading.

2025 RELEASE UNDER E.O. 14176

386. The security system of claim 380 having a plurality of authorized users, and having a means for authorizing for uniquely identifying each of at least one of said authorized users, wherein:

- 5 a particular authorized user initiates said state consistent with presence of an authorized user by activating said means for authorizing using an indicium unique to said particular authorized user; and
10 said user control interface means presents access at said user control interface means to electronic mail message sending from said particular authorized user.

387. The security system of claim 386 wherein:

- said user control interface means comprises keypad means;
5 said indicium comprises a respective passcode unique to each of said at least one authorized user; and
 said activation of said means for authorizing indicium comprises entry of said passcode
10 at said keypad means.

388. The security system of claim 386 wherein:

- said user control interface means comprises means for receiving;
5 said indicium comprises a respective means for transmitting uniquely coded to each of said at least one authorized user; and
 said activation of said means for authorizing unit comprises activation of said coded
10 means for transmitting in communication range of said means for receiving.

SECRET 1330000

389. The security system of claim 388 wherein said means for receiving and said coded means for transmitting are wireless.

390. The security system of claim 99 wherein:
said user control interface means
comprises means for reading a token;

5 said indicium comprises a respective
token uniquely coded to each of said at least one
authorized user; and

said activation of said means for
authorizing comprises presentation of said coded token
to said means for reading.

391. The security system of claim 376
wherein:

said data comprise electronic mail;
said system has at least one authorized
5 user, and has a means for authorizing for uniquely
identifying each of at least one of said authorized
users; and

when one of said at least one authorized
user enters a security system command at said user
10 control interface means by activating said means for
authorizing using an indicium unique to said one of
said at least one authorized user, said user control
interface sends an electronic mail message to a
predetermined recipient advising of said entry of said
15 command by said user.

392. The security system of claim 391
wherein:

said user control interface means
comprises keypad means;

5 said indicium comprises a respective
passcode unique to each of said at least one authorized
user; and

 said activation of said means for
authorizing comprises entry of said passcode at said
10 keypad means.

393. The security system of claim 391
wherein:

 said user control interface means
comprises a means for receiving;

5 said indicium comprises a respective
means for transmitting uniquely coded for each of said
at least one authorized user; and

 said activation of said means for
authorizing comprises activation of said coded means
10 for transmitting in communication range of said means
for receiving.

394. The security system of claim 393 wherein
said means for receiving and said coded means for
transmitting are wireless.

395. The security system of claim 391
wherein:

 said user control interface means
comprises means for reading a token;

5 said indicium comprises a token uniquely
coded to each of said at least one authorized user; and

 said activation of said means for
authorizing comprises presentation of said coded token
to said means for reading.

396. The security system of claim 376
wherein:

11/01/2010 10:00:00 AM

- 10 for transmitting in communication range of said means
for receiving.

399. The security system of claim 398 wherein
said means for receiving and said coded means for
transmitting are wireless.

400. The security system of claim 398
wherein:

said respective means for transmitting
is encoded with multiple codes;

- 5 said activation of said means for
authorizing comprises activation of a selected one of
said multiple codes by said one of said at least one
authorized user; and

- 10 said system retrieves a different World
Wide Web page based on which of said multiple codes has
been selected.

401. The security system of claim 396
wherein:

said user control interface means
comprises means for reading a token;

- 5 said indicium comprises a respective
token uniquely coded for each of said at least one
authorized user; and

- said activation of said means for
authorizing comprises presentation of said coded token
10 to said means for reading.

402. The security system of claim 376
wherein:

- said system has at least one authorized
user, and has a means for authorizing for uniquely
5 identifying each of at least one of said authorized
users;

405. The security system of claim 376

wherein:

said system transmits security data
signals to a central communication station via said
5 external data network and an alternate channel and
awaits acknowledgment thereof; and

when said acknowledgment arrives from a
first one of said external data network and said
alternate channel, said system terminates transmission
10 of said security data on a second one of said external
data network and said alternate channel.

406. The security system of claim 405

wherein:

one of said external data network and
said alternate channel normally operates faster than
5 another of said external data network and said
alternate channel; and

said system begins transmission of said
security data signals on said one of said external data
network and said alternate channel before beginning
10 transmission of said security data signals on said
another of said external data network and said
alternate channel.

407. The security system of claim 405 further
comprising firewall means between said user control
interface means and said external data network;
wherein:

5 said firewall means allows only
communication originating at said system and prevents
communication originating on said external data
network; and

to receive said acknowledgment from said
10 central communication station, said system initiates
communication with said external data network so that

2025 RELEASE UNDER E.O. 14176

said firewall means allows said communication, said initiated communication including a query to said external data network for said acknowledgment to be
15 communicated from said central communication station to said system.

408. The security system of claim 407 wherein said query to said external network comprises a query to said central communication station.

409. The security system of claim 405 wherein said alternate channel is said telephone line.

410. The security system of claim 376 wherein:

said system transmits security data signals to a central communication station via a
5 plurality of channels; and

when said acknowledgment arrives from a first one of said plurality of channels, said system terminates transmission of said security data on each other one of said plurality of channels.

411. The security system of claim 410 wherein:

one of said plurality of channels normally operates faster than others of said plurality
5 of channels; and

said system begins transmission of said security data signals on said one of said plurality of channels before beginning transmission of said security data signals on said others of said plurality of
10 channels.

412. The security system of claim 376 wherein said system accepts commands from a user via said external data network.

413. The security system of claim 412 further comprising firewall means between said user control interface means and said external data network; wherein:

5 said firewall means allows only communication originating at said system and prevents communication originating on said external data network; and

 to receive said commands from said user,
10 said system initiates communication with said external data network so that said firewall means allows said communication, said initiated communication including a query to said external data network for commands issued by said user to be communicated from said external data
15 network to said system.

414. The security system of claim 376 wherein said system sends security data signals to predetermined recipients via said external data network.

415. The security system of claim 376 comprising more than one of said user control interface means, each said user control interface means functioning as an independent terminal of said external
5 data network.

416. The security system of claim 376 further comprising firewall means between said user control interface means and said external data network; wherein:

5 said firewall means allows only
communication originating at said system and prevents
communication originating on said external data
network; and

 to receive data, said system initiates
10 communication with said external data network so that
said firewall means allows said communication, said
initiated communication including a query to said
external data network for data sought to be
communicated from said external data network to said
15 system.

 417. A secure communications system
comprising:

 first communication means connected to a
communication medium;

5 central communication means connected to
said communication medium; and

 at least second communication means
connected to said communication medium; wherein:

 all communication between said first
10 communication means and said central communication
means is initiated by said first communication means;

 communication between said first
communication means and said second communication means
is established by leaving a message for said first
15 communication means at said central communication means
indicating communication is desired between said first
communication means and said second communication
means; and

 when said first communication means
20 initiates communication with said central communication
means, said first communication means receives said
message for said first communication means, maintains
its initiated communication with said central
communication means and instructs said central

2025 RELEASE UNDER E.O. 14176

25 communication means to relay communications between
said first communication means and said second
communication means.

418. The secure communications system of
claim 417 wherein said message for said first
communication means is left by said second
communication means.

419. The secure communications system of
claim 417 wherein said message for said first
communication means is left by said second
communication means.

420. The secure communications system of
claim 417 wherein:

said first communication means includes
a first firewall between said first communication means
5 and said communication medium; and

said first firewall allows only
communication originating at said first communication
means and prevents communication originating on said
communication medium.

421. The secure communications system of
claim 417 wherein:

said first communication means further
comprises first encryption means for encrypting and
5 decrypting communications using a first digital key
identified with said first communication means;

said central communication means further
comprises:

central encryption means for encrypting
10 and decrypting communications using a digital key, and

key memory for storing said first digital key and associating said stored first digital key with said first communication means;

15 said first communication means uses said first encryption means to encrypt with said first digital key each communication sent to said central communication means, and to decrypt with said first digital key each communication received from said central communication means; and

20 said central communication means uses said central encryption means to encrypt with said first digital key each communication sent to said first communication station and to decrypt with said first station digital key each communication received from
25 said first communication station.

422. The secure communications system of claim 421 wherein:

all communication between said second communication means and said central communication
5 means is initiated by said second communication means;

communication between said second communication means and said first communication means is established by leaving a message for said second communication means at said central communication means
10 indicating communication is desired between said second communication means and said first communication means; and

when said second communication means initiates communication with said central communication
15 means, said second communication means receives said message for said second communication means, maintains its initiated communication with said central communication means and instructs said central communication means to relay communications between

20 said first communication means and said second communication means.

423. The secure communications system of claim 422 wherein said message for said second communication means is left by said first communication means.

424. The secure communications system of claim 422 wherein said message for said second communication means is left by said central communication means.

425. The secure communications system of claim 422 wherein:

said second communication means includes a second firewall between said second communication means and said communication medium; and

said second firewall allows only communication originating at said second communication means and prevents communication originating on said communication medium.

426. The secure communications system of claim 422 wherein:

said second communication means further comprises a second encryption means for encrypting and decrypting communications using a second digital key identified with said second communication means;

said key memory of said central communication means further stores said second digital key and associates said stored second digital key with said second communication means;

said second communication means uses said second encryption means to encrypt with said second digital key each communication sent to said

central communication means, and to decrypt with said
15 second digital key each communication received from
said central communication means; and

said central communication means uses
said central encryption means to encrypt with said
second digital key each communication sent to said
20 second communication means and to decrypt with said
second digital key each communication received from
said second communication means.

427. The secure communications system of
claim 426 wherein:

said first communication means is a
premises alarm system; and

5 said second communication means is a
central alarm monitoring station.

428. The secure communications system of
claim 426 wherein:

said first communication means is a
first premises alarm system; and

5 said second communication means is a
second premises alarm system.

429. The secure communications system of
claim 426 wherein:

said first communication means is a
premises alarm system; and

5 said second communication means is a
remote communications terminal.

430. The secure communications system of
claim 417 wherein:

all communication between said second
communication means and said central communication

5 means is initiated by said second communication means;

100-100000-100000

communication between said second
communication means and said first communication means
is established by leaving a message for said second
communication means at said central communication means
10 indicating communication is desired between said second
communication means and said first communication means;
and

when said second communication means
initiates communication with said central communication
15 means, said second communication means receives said
message for said second communication means, maintains
its initiated communication with said central
communication means and instructs said central
communication means to relay communications between
20 said first communication means and said second
communication means.

431. The secure communications system of
claim 430 wherein said message for said second
communication means is left by said first communication
means.

432. The secure communications system of
claim 430 wherein said message for said second
communication means is left by said central
communication means.

433. The secure communications system of
claim 430 wherein:

said second communication means includes
a second firewall between said second communication
5 means and said communication medium; and

said second firewall allows only
communication originating at said second communication
means and prevents communication originating on said
communication medium.

434. The secure communications system of claim 430 wherein:

said first communication means is a premises alarm system; and

5 said second communication means is a central alarm monitoring station.

435. The secure communications system of claim 430 wherein:

said first communication means is a first premises alarm system; and

5 said second communication means is a second premises alarm system.

436. The secure communications system of claim 430 wherein:

said first communication means is a premises alarm system; and

5 said second communication means is a remote communications terminal.

437. The secure communications system of claim 417 wherein:

said first communication means is a premises alarm system; and

5 said second communication means is a central alarm monitoring station.

438. The secure communications system of claim 417 wherein:

said first communication means is a first premises alarm system; and

5 said second communication means is a second premises alarm system.

439. The secure communications system of claim 417 wherein:

said first communication means is a premises alarm system; and

5 said second communication means is a remote communications terminal.

440. The secure communications system of claim 417 further comprising:

at said central communication means, at least one service agent means for communicating between
5 said first communication means and at least one service on said communications medium; wherein:

at least one of said at least one service requires a secure identifier for access thereto; and

10 at least one of said at least one service agent means comprises means for securely storing an identifier, a user at said first communication means registering said user's secure identifier for said at least one of said at least one
15 service; whereby:

when said user accesses said at least one of said at least one service, said user need not transmit said secure identifier over said communication medium, said secure identifier being transmitted
20 securely by said service agent means from said secure identifier storage means.

441. A secure communications system for communicating between first and second communication means connected to a communications medium; said system comprising:

5 a central communication means connected to said communication medium and having a secure digital session key generating means; wherein:

each of said first and second
communication means further comprises a respective
10 encryption means for encrypting and decrypting
communications using a digital key;
all communication with said first
communication means is initiated by said first
communication means;
15 all communication with said second
communication station is initiated by said second
communication means;
communication between said first
communication means and said second communication means
20 is established by generating at said secure digital
session key generating means a secure digital session
key and leaving a respective message at said central
communication means for each of said first and second
communication means, each said respective message
25 including said secure digital session key;
when said first communication means
initiates communication with said central communication
means, said first communication means receives said
message including said secure digital session key;
30 when said second communication means
initiates communication with said central communication
means, said second communication means receives said
message including said secure digital session key; and
said first and second communication
35 means communicate with one another using said secure
digital session key and said respective encryption
means.